Analysis of Android Smart Watch Artifacts

Shreyas Parikh[1], IFS, GFSU, Dhaval Chavda[2], IFS, GFSU, Shourjo Chakraborty[3], SysTools Software Pvt. Ltd.
Dr. Parag H. Rughani[4], IFS, GFSU, Dr. M. S. Dahiya[5], IFS, GFSU

Abstract— Innovations of smart phones have made this era as an era of smart devices. People are using smart phones more than any other device / tool in their day-to-day life. Since, android entered to this market, use of wearable devices became possible technically and economically. These days, wearable devices like wrist band, earring, smart watch, smart shoes, etc. have become easily available and affordable. Android based smart watch is one of such popular devices being used by many people around the world. Though the watch is dependent on android smart phone, it contains lots of useful information about user. The user information stored on the device can be important in tracing any cyber crime / traditional case. This paper discusses what information the Android Smart Watch sores and analysis of this information from forensics point of view.

Index Terms— Android Forensics, Smartwatch Forensics, Wearable Forensics, Android Smartwatch, Android Smartwatch Artifacts, Android Analysis, Artifact Analysis.

1 INTRODUCTION

As per emarketer survey there are estimated 1914.6 million people owned a smartphone[1]. The major platforms in the current smartphone market are Google's Android with almost eighty percent of the market, Apple's iOS with sixteen percent and Microsoft's Windows Mobile OS with three percent.

This shows Google's Android operating system owns the largest portion of smart phone market. With the aim of integrating all digital platform with smart OS, Google took its first step by introducing Android wear last year in March 2014 to step into wearable market.

With the introduction of the smart watch to the family of wearable computing devices by Android, Smart watches are now seen to be socially acceptable in the modern digital world, and can possibly be used as an alternative interface for information access.

Since, smart watches can be used as an interface for operating and accessing smart phones, the use is expected to increase in near future. This handy gadget will be on the wrists of many people in coming days. As the usage will increase possibilities of number of crimes related to smart watch may also increase.

Looking at the prospectus feature, we can not neglect possibilities of required investigation of Smart watch found from a crime scene. The smart watch can become a very strong evidence in solving a crime. Since it can contain lots of information, it may become one of the important evidence which can reveal useful information related to a victim or suspect.

This work focuses on extraction and investigation of possible sensitive artifacts from smart watch to prove relevance with the case. Main objective of this work is to extensively explore possible locations from where sensitive information as well as information conveyed through communication channels like Bluetooth can be retrieved.

- *Shreyas Parikh, First Author has completed his M. S. in Digital Forensics and Information Assurance from GFSU, India, E-mail: shreyas.prkh@gmail.com*
- *Dhaval Chavda, Second Author has completed his M. S. in Digital Forensics and Information Assurance from GFSU, India, E-mail: er.dhaval.chavda@gmail.com*
- *Dr. Parag H. Rughani, Corresponding Author Assistant Professor in Digital Forensics and Cyber Security at GFSU, India, E-mail: parag@gfsu.ac.in*

2 WEARABLE COMPUTING

2.1 Background

The concept of wearable computing emerged during mid of 90's. At that time, carrying an "always- on" computer with head mounted display and control interface became practically possible.

Reduced size of hardware components, availability of low cost sensors and existence of widespread Internet access, allowed wearable computing devices to become more commonplace, readily wearable and socially acceptable. "This energetic expansion of miniature computing devices has led to the concept of The Internet of Things (IoT) which can be described as a collection of interconnected and interactive devices which are able to communicate useful real-time information between one another" (Swan, 2012) [2].

The smart watch falls in the category of the Internet of Things, which acts as a peripheral device to a connected smart phone. By establishing connection between smart watch and smart phone, one can easily operate and use smart phone through smart watch.

2.2 Android Smart Watch (Android Wear)

Smart Watch is a device that maintains persistent connectivity (wireless connection) to your mobile devices - usually a smart phone and can also receive notification like calls, social updates in terms of notification, instant messages and more.

On 18 th March 2014 Google Official Announced that they are coming for another arena into the world of Wearable Technologies with Android Wear, A New Operating System for Wearable Devices.

The Android Wear operating system uses Bluetooth communication to connect hand-held device(s). Prerequisite of operating system is, it requires hand-held device running on version Android 4.3 or higher and one companion application to synchronize data with device.[3]

Once connection is initiated, the wearable channels information and updates it from paired device, and comfortably displays them on the customer's wrist.

These updates include things like Gmail, Google Calendar, Google Now cards, and phone notifications, such as incoming calls and text messages. Android Wear is a wearable devices/gadget which keeps user's hands free and yet allows user to use his/her smart phone.

2.3 Wearable APIs

Basic Structure of Android Wear (Smart Watch and Google Glass) is similar to Android OS structure. As well the Kernel is also same as Android Operating System. Wearable data layer is used to handle lots of complex and complicated data in timely manner by interacting with smart phone.

Basic structure of Android Wear is mainly based on three APIs.

- Data API
- Message API
- Node API

Node API: The Node API informs to smartphone when a node is connected. Node events are delivered to every application on devices.

Message API: The Message API manages API calls between devices.

Data API: The Wearable Data Layer API, which is part of Google Play services, provides a communication channel for the hand-held and wearable apps. The API consists of a set of data objects that the system can send and synchronize over the wire and listeners that notify the apps of important events with the data layer.

Saminath explained communication between Android Wear and Android Phone in his work as: "communication between the Android Handheld device and Wearable Device. Wearable API gets reference from connected mobile device. Data Layer API supports syncing data between handheld and wearable devices.

Wearable Listener interface pulling the notifications from paired Android Smartphone's or tablets and display text using Message API. Message API is a one-way communication mechanism that's meant for 'fire-and-forget' tasks". This is just opposed to Wear's Data Layer API. The Google Play service will make this very easy. The communication between two apps over the Bluetooth link that pair two devices" [5]

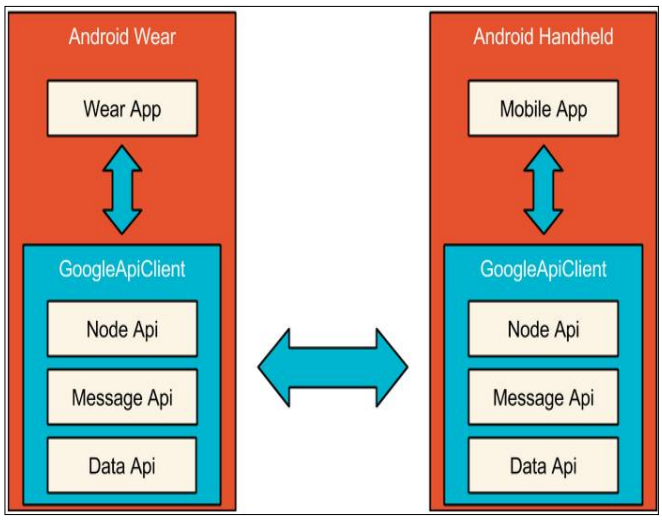

Fig. 2.3.1. Android Wear API Structure [4]

3 NEED OF DIGITAL FORENSICS OF SMART WATCH

Number of cyber crimes are increased day by day and criminals use latest tools and technologies for committing sophisticated crimes. As per the Symantec's Internet Security Threat Report published in April, 2015.

"Symantec expects to see further malware development and attacks on the Internet of Things as criminals find new ways to make money from doing so. For example, some attackers have used Darlloz to mine for crypto-currencies similar to bitcoins. Other attackers have leveraged hacked routers to carry out distributed denial-of-service attacks. Experience with PCs and, more recently, witn mobile malware suggests that where there is opportunity created by technical exploits and motivation, such as greed, vindictiveness, or revenge, there will be cyberattacks."[6]

This not only predicts increase in number of attacks on IoT, it also alerts Cyber Security Experts and Forensic Experts to equip themselves for upcoming threats. Even though, prevention is better than cure, it is not completely possible to mitigate attacks. The incident response and forensic analysis of a crime / attack is equally important and required as securing a network.

This work emphasis mainly on recovering important artificats from Android Smart Watch, which may help Forensic Investigators in collecting information about Victim(s) and / or Criminal(s) related to the case.

4 METHODOLOGY

The experiment was carried out on a rooted Sony Smartwatch 3 (model # SW50) running android wear version 5.0.2 OS.

We used android SDK, FTK and Hex Editor to carry out the work.

4.1 Acquisition

Creating image of evidence is one of the most important tasks in any digital forensic investigation, because the thumb rule of forensic investigation says that you cannot work on actual evidences. For that we have to create bit by bit image of the target device or evidence in terms of forensics. For checking integrity of the evidence we should make sure that hash is calculated before starting the imaging of evidence or original data. We also need to verify it with the calculated hash of image. Further, to avoid any accidental modifications during the imaging process, the evidence device should be in write protected mode.

Android wear device stores information at different places within /dev partition. With the help of MTD of Linux kernel it stores memory chunks in running OS with names like "mmcblk[#]p[#]"

The command ls -al /proc/partition with su from adb shell will generate following output.

Fig. 4.1.1. Memory Chunks

First line of above output is:

abi -> /dev/block/mmcblk0p1

Which indicates the abi partition data/information is stored in mmcblk0p1 memory block. Similarly different partitions like /boot, /system, /cache, /ram, /apps-log, etc and their relevant memory blocks can be seen from the same output. So for understanding what type of data a block can store one has to carve out that particular memory block.

For example, following command can be used to carve data from memory block /dev/block/mmcblk0p1 which refers to partition /abi.

dd if = /dev/block/mmcblk0p15 of=/sdcard/download/versioninfo.dd

Similarly, other blocks can be carved and separate dd image of each can be created for analysis.

4.2 Image Analysis

The paper discusses analysis of the main three images which are crucial as well as complex in any android device investigation. These images are of cache memory, system memory and userdata memory.

4.2.1 Cache

Cache partition contains cached data of a particular application in android that helps device to accelerate performance. In our case, wear device gathers information of various logs inside cache partition like recovery, system and partition logs. For example recovery folder contain recovery information for various partition and other system files. This logs are appended and denoted with 'last_log.x' where x is appended file number.

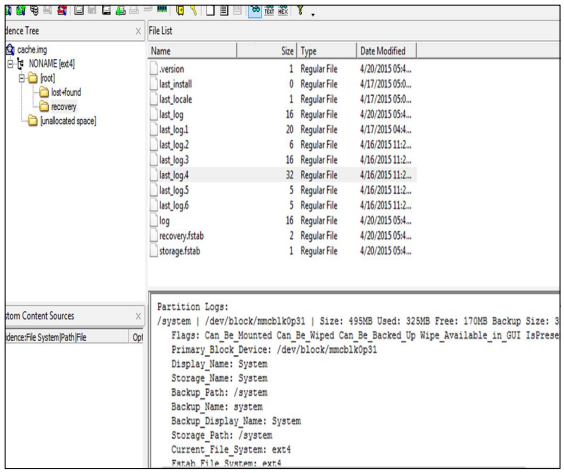

Fig. 4.2.1.1. Cache Image

4.2.2 System Image

System partition contains information about core system such as installed applications, media files, OEM Applications, fonts, framework etc. Command, ls –al can be used to see which memory block contains information about system partition.

Here in our case the partition is mapped with block mmcblk0p31. Following image displays tree structure of ext4 file system partition.

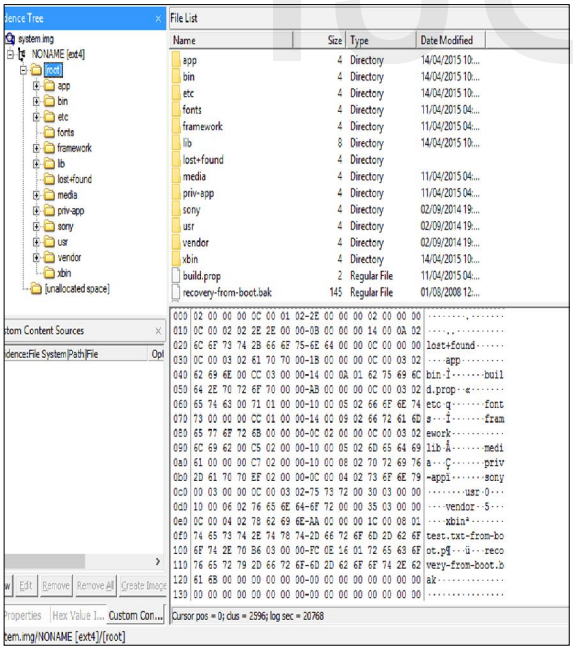

Fig. 4.2.2.1. System Image

4.2.3 Data Image

This is where user data is stored. This includes everything from user settings & customizations, apps that you have downloaded and installed, your messages (SMS / MMS) as well as contacts.

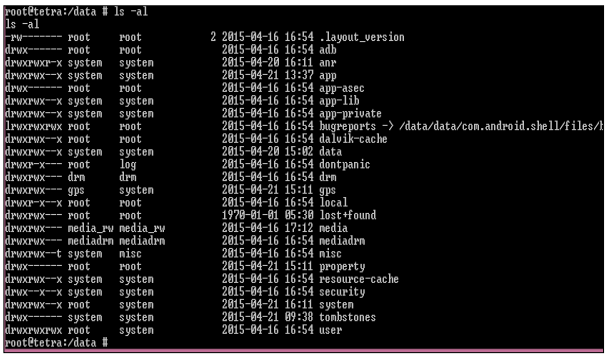

Fig. 4.2.3.1. Data Image

Wiping data partition will restore your phone to factory settings, removing all apps, messages and user settings from the device[7].

This folder has significant importance in investigation as it holds the valuable information. This is the partition that contains most of the data that belongs to user. The following screenshot displays current folder inside partition. Some of the important subdirectories under data folder are: App, Dalvik-cache, Data, Misc, Property and system.

4.3 Important Artifacts

From our experiment we have found few important artificats, analysis of some of them are discussed below.

4.3.1 Paired Device Information

Paired device information is located inside /data/misc folder. It contains five subdirectory in which one of it is bt_config. This file gives information about connected Bluetooth device with device id and mac address, as shown in following figure.

Fig. 4.3.1.1. Paired Device Info.

4.3.2 Voice Commands

Smart watch is operable through voice commands. This voice commands are transmitted via google gms service. This commands are also stored on the connected device and synced with respective google account. This gms service related information can be found inside /data/data/ and as a com.google.android.gms subdirectory. Commands that are triggered to perform various task can be identified by looking up for "voice_action_title".

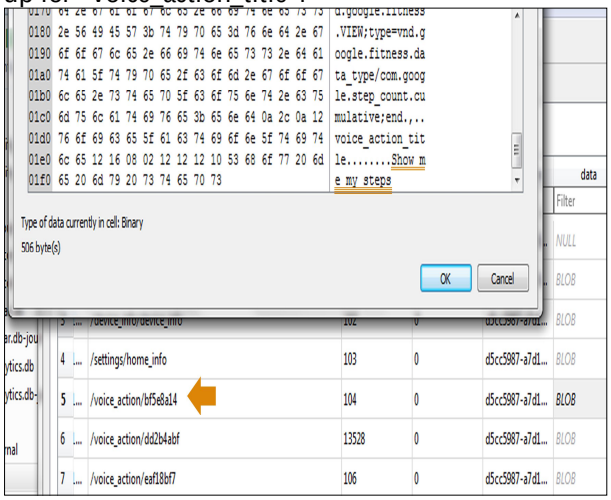

Fig. 4.3.2.1. Voice Commands

4.3.3 Bluetooth Packet Analysis

Device uses Bluetooth v4 or v4 LE (Low Energy). It requires 6 digit pass key to connect with host (android wear). But focusing on transmission packets that are transmitted to other device, is in plain text format making it easily readable and this packets can be captured via any network/Bluetooth packet capturing software.

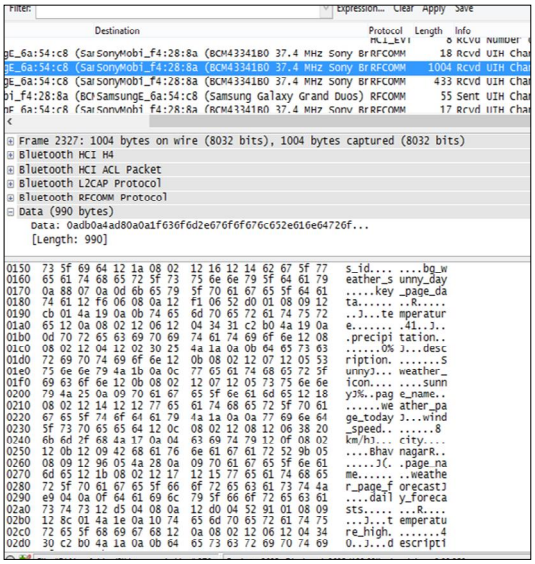

Fig. 4.3.3.1. Bluetooth Packet Analysis

4.3.4 Logcat

The Android logging system provides a mechanism for collecting and viewing system debug output. Logs from various applications and portions of the system are collected in a series of Circular buffers, which then can be viewed and filtered by the logcat

command.(Source: Android developer forum)

So we can use Logcat to view different system events like verbose message, debug message, information regarding process, warning and system errors.

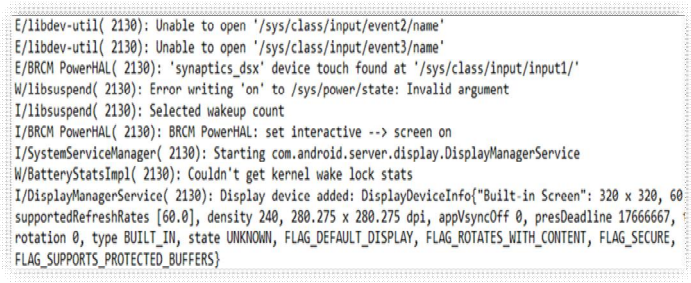

Fig. 4.3.4.1. Logcat

4.3.5 Notifications

Application notifications are transmitted to base device via Google gms service. Investigating this directory can revel database with application name and notification. Following screenshot is example of Whatsapp notification received on device with sender number.

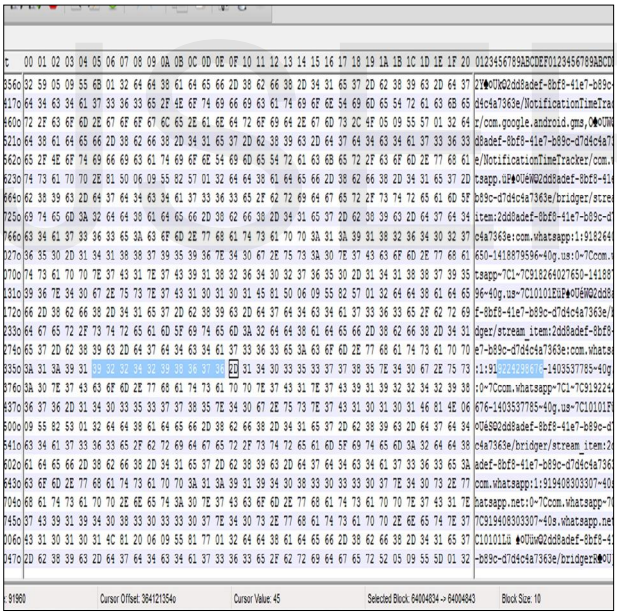

Fig. 4.3.5.1. Notifications (WhatsApp Details)

4.3.6 DropBox Artifacts

The Dropbox Folder located under /data/system/ contains information about synchronize time (start and end time in Unix Timestamp with 13 digit number) with log detail as shown in following figure.

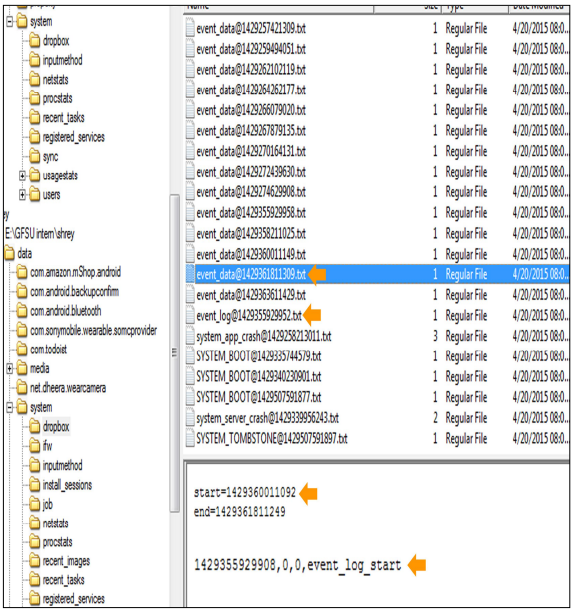

Fig. 4.3.6.1. DropBoxArtifacts

4.3.7 Recent Tasks

The Recent task folder stored under /data/system/ contains list of tasks in xml format. It creates separate file for each task. Following figure shows information about 21_task.xml.

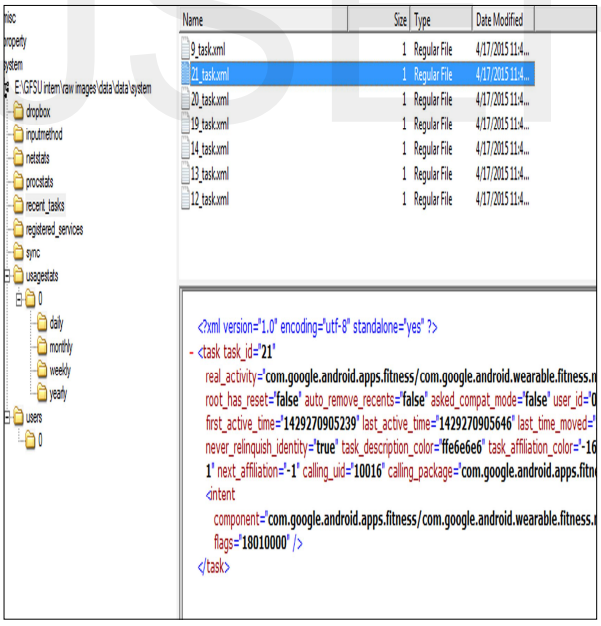

Fig. 4.3.7.1. Recent Tasks

It contains useful information like package name, first active time, last active time, etc.

5 FUTURE SCOPE

The work can be further extended to forensically analyse smart watches from other manufacturers like Apple, Microsoft, Blackberry, etc. The researchers can continue working on the same techniques for retrieving data from other Android Wearable Devices.

6 CONCLUSION

The techniques discussed in this paper may assist Forensic Investigators in analysing Android based Smart Watch. The researchers can use this as a first step to find out other techniques for the same family of wearable devices.

REFERENCES

[1] http://www.emarketer.com
[2] http://www.swan-forum.com/swan-2012-conference.html
[3] http://www.android.com/wear/
[4] http://swarmnyc.com/whiteboard/building-android-wear-watch-face-with-live-weather-data-3/
[5] Saminath, "Power of Android Wearable Technology", International Journal of Scientific and Research Publications, Volume 5, Issue 2, February 2015.
[6] https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf
[7] http://en.miui.com/thread-12612-1-1.html